

MAG-UX

Visualize your performance & security

IT 비즈니스 구성 요소에 대한 효과적인 장애 모니터링 방안

An Effective Failure Monitoring Plan for IT Business Components





Performance Monitoring
성능 모니터링

Visualize your performance & security

Security Monitoring
보안 모니터링

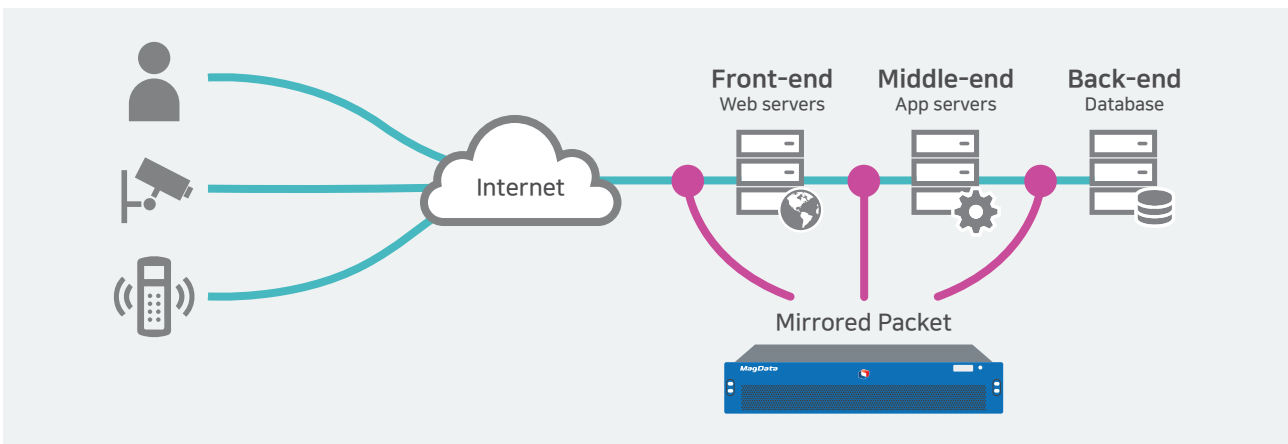


IT 비즈니스 구성 요소에 대한 효과적인 장애 모니터링 방안

맥데이터 MAG-UX

복잡하고 다양해진 디지털 비즈니스 환경에서 IT 구성 요소에 대한 장애는 전체 비즈니스를 마비시킬 수 있는 정도이기에 매우 중요한 해결 대상이다. 따라서 어플리케이션, 네트워크, 그리고 서버를 포함하는 각종 인프라 장비들에 대한 성능과 보안적 측면의 장애를 보다 빠르게 진단하고 장애 요소를 해결하는 것이 요구된다. 특히, IoT의 급속한 발전에 따라 더욱 복잡해진 네트워크와 대규모 장치들에 의한 다양한 트랜잭션들은 장애를 유발시킬 가능성을 극대화시키고 있는 것이 현실이다. 데이터 센터를 포함한 클라우드 센터, 홈 IoT, 스마트 팩토리, 그리고 스마트 시티 등의 급속한 발전으로 장애를 감지해야 할 대상은 기하급수적으로 증가 추세이며, 모든 디지털 비즈니스 기업들은 정확한 장애 감지를 위한 기술적 방안을 반드시 수립해야 할 시점이다.

맥데이터의 MAG-UX는 복제된 패킷에 대한 고성능 심층 패킷 분석 기술에 기반한 네트워크 수준에서의 성능 및 보안적 측면의 장애 감지 기능을 제공하고 있다. 이 기능을 수행하기 위하여 MAG-UX는 네트워크의 와이어 데이터를 L7 수준으로 실시간 해석하여 장애 상황을 빠르게 식별 및 분석하여 IT 구성 요소 구간간에 대한 가시성과 직관성을 제공한다.



<그림 1> 고성능 패킷 분석 기술에 기반한 구간별 장애 진단

※ **와이어 데이터** (Wikipedia, https://en.wikipedia.org/wiki/Wire_data)

Wire data is the information that passes over computer and telecommunication networks defining communications between client and server devices. It is the result of decoding wire and transport protocols containing the bi-directional data payload. More precisely, wire data is the information that is communicated in each layer of the OSI model.

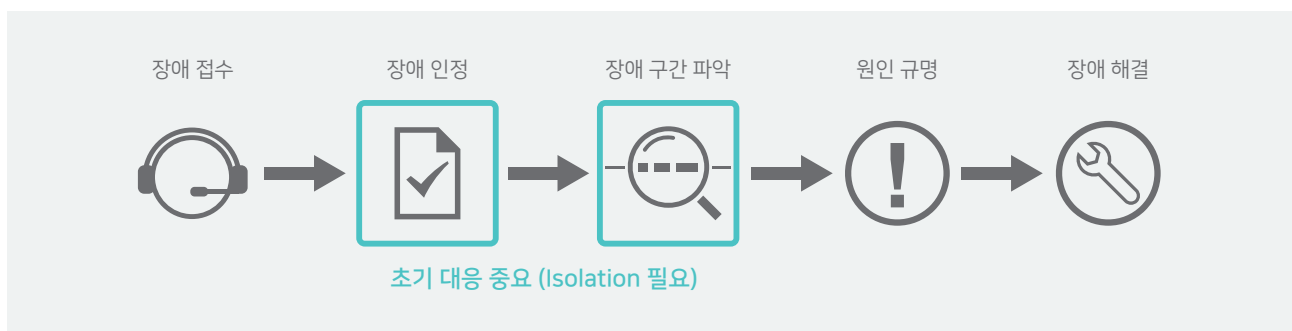
장애의 정의

일반적으로 널리 인식되어 있는 IT 비즈니스 구성 요소의 장애 원인은 성능적 측면의 비의도적인 장애이다. 예를 들면, 웹 서비스를 위한 서버가 프로그램의 버그 또는 설계 오류로 대규모의 사용자 요청을 처리하지 못하고 10초 이상 대기하는 상황을 발생시키거나, IP 카메라가 관리자의 실수로 불필요한 과대 트랜잭션을 중앙 서버로 발생시켜 중앙 서버가 과부하가 걸리는 상황이 발생하는 것이 바로 그것이다. 참고로 이런 예들은 사용자 관점에서 서비스 장애로 판단되는 것이다. 그러나, 전체적 관점에서 장애를 정의하자면 성능적 측면의 장애와 보안적 측면의 장애로 구분되며, 이 두 장애 구분은 의도적 장애 원인과 비의도적 장애 원인으로 세분화된다. 특히 의도적 장애 원인인 사이버 공격은 구성 요소의 성능을 떨어뜨리는 현상을 발생시켜 성능적 측면의 장애 상황을 일으킨다.

	의도적 장애 원인	비의도적 장애 원인
성능적 측면	사이버 공격	시스템 설계 오류 시스템 동작 오류 관리자 실수
보안적 측면	사이버 공격 해킹	

<그림 2> IT 비즈니스 구성 요소의 장애 구분

MAG-UX의 경우 성능과 보안이라는 양측면의 의도적 장애와 비의도적 장애를 폭넓게 감지할 수 있는 기능을 탑재하고 있으며, 신속한 장애 구간을 파악하기 위한 가시성과 직관성을 제공한다. 그러나, MAG-UX는 보안적 측면의 장애를 감지하는 새로운 개념적 기능을 제공하는 것이지 종래의 IPS와 같은 보안 솔루션을 대체할 수 있는 것은 아니다.



<그림 3> IT 비즈니스 구성 요소의 장애 처리 프로세스

가시성과 직관성

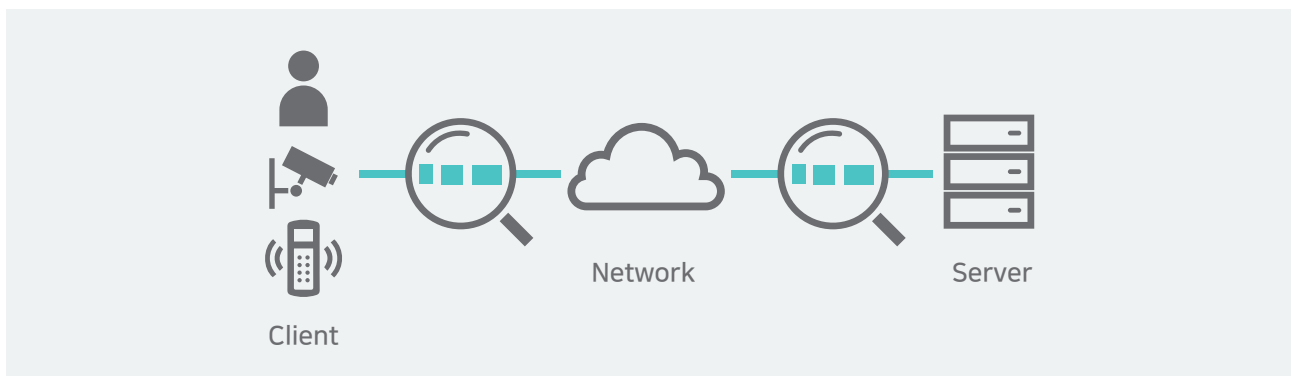
글로벌 최고 수준의 IT 컨설팅 기업인 Gartner가 2018년 2월 21일에 발표한 자료("Magic Quadrant for Network Performance Monitoring and Diagnostics")에 따르면, NPMD 솔루션의 목표는 IT 구성 요소에 대한 중단 및 성능 저하 해결을 용이하게 하기 위해 네트워크 트래픽 및 인프라를 모니터링하는 것뿐만 아니라 성능 최적화 기회를 식별하기 위한 것이라고 정의하고 있다. 또한, 보안 운영팀의 네트워크 트래픽 분석에 대한 관심이 높아짐에 따라 여러 NPMD 솔루션 업체가 사이버 보안 시장으로 진출하고 있다고 보고하고 있다. 이러한 NPMD가 제공하는 성능 및 보안적 장애 요소 모니터링 기능들은 진단(diagnostics), 분석(analytics), 그리고 근본 원인 분석 능력(root cause analysis capabilities)에 의해 수행된다고 해당 자료는 설명하고 있다.

이러한 시장적 요구에 발맞추어 MAG-UX는 인프라 모니터링, 성능 최적화 기회, 그리고 보안 모니터링에 대한 가시성을 제공하기 위하여 실시간 모니터링을 통해 설정된 임계치에 도달하면 경고 및 알림을 제공하며 이 기능으로 쉽고, 빠르고, 직관적으로 성능 및 보안 진단이 가능하다.



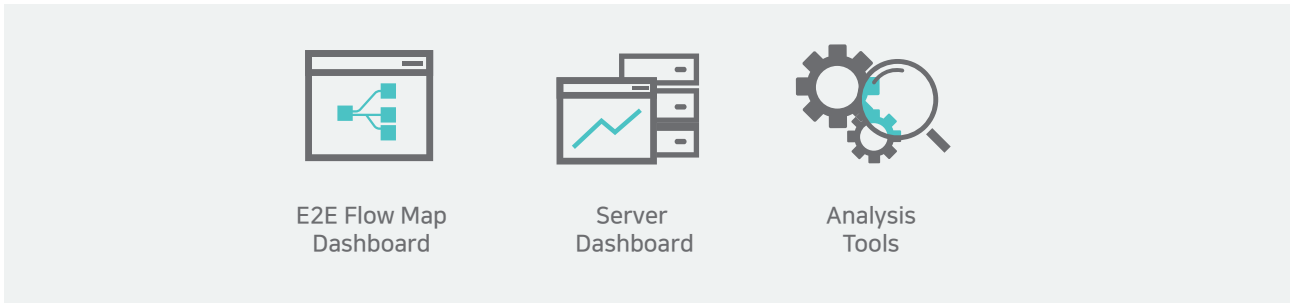
<그림 4> MAG-UX의 실시간 처리 기능

또한, MAG-UX는 각 요소뿐만 아니라 직관적인 각 구간별 상태 분석, 경고 및 알림을 제공하며, 이 기능으로 장애가 되는 문제 구간의 장애 요소를 실시간으로 파악할 수 있다. 이러한 기능적 특징은 MAG-UX가 구간별 스위치 미러링에 의한 특징으로 얻어지는 결과로써, 서버에 부하를 주는 에이전트를 설치하지 않고, 인위적인 패킷을 생성하여 모니터링하지 않으며, 실시간 처리가 어려운 SNMP 혹은 플로우 데이터 방식을 사용하지 않고, 보안 문제가 발생할 수 있는 스크립트 인젝션 방식을 사용하지 않도록 구현되어 있기에 가능하다.



<그림 5> MAG-UX의 구간별 처리 기능

마지막으로, MAG-UX는 다양한 대시보드와 실시간 분석도구를 통해 장애 요소 및 원인 예측 기능을 제공하며, 이 기능으로 전체 관점(IT Control Tower)으로 서비스 성능 진단 및 보안 진단이 가능하게 한다. MAG-UX가 정의하고 주장하는 "IT Control Tower"는 IT 서비스 인프라 성능 평가 분석, 실시간 모니터링, 모든 요소에 대한 분석, 전체 구간에 대한 분석, 쉽고 빠른 의사 결정 도구, 장애 요소 증가 없는 적용, 이상 징후 파악이라는 총 7개의 특징을 갖는다.



<그림 6> MAG-UX의 진단 분석 기능

맺음말

MAG-UX를 개발하는 주식회사 맥데이터는 "Visualize your performance & security"라는 비전으로 와이어 데이터를 분석하여 네트워크 데이터에 가시성과 직관성을 제공하는 기술을 개발하고 있다. 이에 따라 성능 진단(performance monitoring)과 보안 진단(security monitoring)을 주요 핵심 솔루션 영역으로 선정했다. 주력 제품인 MAG-UX는 2012년부터 개발을 시작하여 다양한 고객의 요구를 수렴하며 진화하였으며, 서버를 대상으로 시작된 기술은 IoT 장치로 확대 발전되어 초연결시대를 위한 기술로 발전 중이다. 또한, Trillion급 빅데이터 처리 기능을 제공하기 위하여 다중 병렬분산 아키텍처 기반의 초대용량 처리를 지원할 수 있는 MAG-UX 기술을 개발 중이고, Anomaly Detection 기능을 제공하기 위하여 실시간으로 수집되는 각종 데이터를 Heuristic에 기초한 인공지능(AI) 기법으로 분석하는 MAG-UX 기술을 개발하고 있다. 따라서, MAG-UX가 IT 비즈니스 구성 요소에 대한 효과적인 장애 모니터링 방안을 제공할 것임을 확신한다.

※ NPMD (Gartner, <https://www.gartner.com/reviews/market/npm>)

Network performance monitoring and diagnostics tools enable IT and network operations teams to understand the ongoing behavior of the network and its constituent elements in response to traffic demands and network utilization. Measuring and reporting on network performance is crucial to ensuring that performance stays at an acceptable level. Customers in this market are looking to identify tools to detect application issues, identify root causes and perform capacity planning.



MAG-UX

Visualize your performance & security

Function

Real-Time Processing

Sectional Processing

Diagnosis & Analysis

Feature

IT Control Tower

Port Mirroring(Agentless)

Transaction (L7) Analysis

MAG-UX

Visualize your performance & security



Easy



Real-Time



Intuitive

MAG-UX는 IT 서비스 인프라에 대한 성능 진단 및 보안 진단을 위하여 서비스 전구간에 대한 가시성과 직관성을 제공하며, 이 기능으로 서비스 장애에 대한 요소 및 구간 파악이 가능합니다.

주식회사 맥데이터 **MagData Inc.**

서울특별시 영등포구 당산로41길 11, SK V1센터 W동 1007-B(우07217)
W-1007B, 11, Dongsan-ro 41-gil, Yeongdeungpo-gu, Seoul, 07217, Rep. of Korea

+82-(0)2.6121.8470

+82-(0)2.6121.8471

magdata.net

contact@magdata.net

MagData 